UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,890	09/28/2001	E. David Neufeld	COMP:0224	4334

7590   07/01/2005

Intellectual Property Administration
Legal Dept., M/S35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER
TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/966,890	NEUFELD ET AL.
	Examiner	Art Unit
	Tamara Teslovich	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>28 September 2001</u>.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-32</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-32</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>28 September 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date <u>04.15.02</u>.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

5   The specification shall conclude with one or more claims particularly pointing out and distinctly
       claiming the subject matter which the applicant regards as his invention.

Claim 26 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

10   regards as the invention.

Claim 26 recites the limitation "the second type of triggering event" in line 3.

There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

15   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

       A person shall be entitled to a patent unless –

       (b) the invention was patented or described in a printed publication in this or a foreign country or in public
       use or on sale in this country, more than one year prior to the date of application for patent in the United
20   States.

Claims 1-7, 12, 19-24, and 26 are rejected under 35 U.S.C. 102(b) as being

anticipated by Bruce Schneier's "Applied Cryptography", hereinafter referred to

25   **as *Schneier*.**

Regarding claim 1, Schneier discloses a method of generating a random number
for a cryptographic security subsystem of a processor-based device, the method
comprising the acts of (a) detecting occurrences of a first type of triggering event (page
426 lines 6-14); (b) writing one or more bits of data to a seed pool (or reservoir) upon

5   termination of the first type of triggering event (page 426 lines 8-9); and (c) repeating
acts (a) and (b) until (enough events have taken place) the seed pool is full (page 428
lines 16-18).

Regarding claim 2, Schneier further discloses the act of capturing one or more

10   bits of data from a free-running timer (most finely grained time-of-day clock, for example
the Intel 8254 clock chip) upon termination of the first type of triggering event (page 426
lines 27-34).

Regarding claim 3, Schneier further discloses that the first type of triggering

15   event has a variable duration (seemingly random events) (page 426 lines 7-8).

Regarding claims 4-6, Schneier further discloses that the processor-based
device is coupled to a communication link, and includes the act of receiving a
communication from the communication link (arrival times of network packets), the link

20   comprising a plurality of types (network, multimedia, etc) (page 426 lines 14-27).

Regarding claim 7, Schneier further discloses (a) detecting occurrences of a

second type of triggering event (a whole lot of seemingly random events); (e) writing

one or more bits of data to the seed pool upon termination of the second type of

triggering event; and (f) repeating act (e) each time the second type of triggering event

5   is detected (for example, hashing together the sector number, time of day, and seek

latency for every disk operation) (page 426 lines 16-17).

Regarding claim 12, Schneier further discloses that the seed pool comprises a

state bit indicative of a state of the seed pool, and wherein the method comprises the

10   act of examining the state bit to determine whether the seed pool is full (waiting until

enough external random events have taken place before continuing) (page 428 lines

16-18).

Claim 19 is directed towards a device's implementation of the method of claim 1

15   and is rejected by similar rationale.

Claim 20 is directed towards a device's implementation of the method of claim 7

and is rejected by similar rationale.

Claim 21 is directed towards a device's implementation of the method of claim 2

and is rejected by similar rationale.

20   Claim 22 is directed towards a device's implementation of the method of claim 3

and is rejected by similar rationale.

Claim 23 is directed towards a device's implementation of the method of claim 4

and is rejected by similar rationale.

Claim 24 is directed towards a device's implementation of the method of claim 5

and is rejected by similar rationale.

5   Claim 26 is directed towards a device's implementation of the method of claim 11

and is rejected by similar rationale.

Claims 13-18, 25, and 27-32 are rejected under 35 U.S.C. 102(b) as being

10   **anticipated by Utz et al., US Patent No. 5,680,131, hereinafter referred to as Utz.**

Regarding claim 13, Utz discloses a method of initializing a seed pool for

generating a random number for a cryptographic security subsystem of a processor-

based device, the method comprising the acts of (a) writing a plurality of bits of data to a

15   seed pool (RS/PRNG), the plurality of bits of data having a signature (start) value (col.5

lines 34-42; col.6 lines 13-28); (b) detecting occurrences of a first type of triggering

event and (c) writing one or more bits of data to the seed pool upon termination of the

first type of triggering event, the one or more bits of data altering the signature value of

the seed pool (col.6 lines 37-61); and (d) enabling the cryptographic security subsystem

20   when more than a predetermined portion of the signature value of the seed pool has

been altered (col.7 line 61thru col.8 line 13; col.9 line 62 thru col.10 line 16).

Regarding claims 14 and 15, Utz discloses wherein the first type of triggering

event comprises either a cycle of power applied to the processor-based device or a

reboot of the processor-based device (power-on reset circuit) (col.5 lines 57-67).

5   Regarding claim 16, Utz discloses wherein act (c) comprises the act of masking

(serially combining) the one or more bits of data into the seed pool (col.6 lines 57-61;

col.5 line 22).

Regarding claim 17, Utz discloses wherein act (c) comprises the act of capturing

10   the one or more bits of data from a free-running timer (clock signals) (col.5 lines 59-61) .

Regarding claim 18, Utz discloses detecting a second type of triggering event;

determining if the seed pool is full; and writing one or more bits of data to the seed pool

upon termination of the second type of triggering event if the seed pool is not full (col.3

15   lines 38-40; col.11 lines 51-55).

Regarding claim 25, Utz discloses wherein the interface controller

comprises an RS232 interface controller (col.7 lines 41-45; col.10 lines 48-53).

20   Regarding claim 27, Utz discloses a processor-based device comprising:

a host processing system, the host processing system comprising a processor

and a communications management system in communication with the host processing

system (col.5 lines 52-67); and

a memory system in communication with the host processing system and the

5   communications management system, wherein the communications management

system comprises: an interface controller (col.6 lines 8-12); a non-volatile memory

device to store a seed pool comprising a plurality of data bits (col.5 lines 34-42); and

security logic in communication with the interface controller and the non-volatile

memory device, the security logic configured to establish a secure communication

10   session between the processor-based device and an external device in communication

with the processor-based device via the interface controller (col.4 lines 47-60), and

wherein the security logic is configured to:

determine whether the plurality of data bits in the seed pool has at least a portion

of a signature value; and disable establishment of the secure communication session if

15   the plurality of data bits has at least a portion of the signature value (col.9 line 62 thru

col.10 line 16).

Regarding claim 28, Utz discloses wherein the security logic is configured to

detect a first type of triggering event, and to write one or more data bits to the seed pool

20   upon termination of the first type of triggering event (col.6 lines 37-61).

Regarding claim 29, Utz discloses a main power supply to supply power to the

processor-based device, and wherein the first type of triggering event comprises a cycle

of the power supplied by the main power supply (power-on reset circuit) (col.5 lines 57-

67).

5

Regarding claims 30-31, Utz discloses wherein the security logic is configured to

detect a second type of triggering event; determine whether the seed pool is fully

populated; and write one or more data bits to the seed pool upon termination of the

second type of triggering event if the seed pool is not fully populated (col.3 lines 38-40;

10   col.11 lines 51-55) and wherein the second type of triggering event comprises receipt of

a communication from the external device via the interface controller (col.3 lines 38-40;

col.11 lines 51-55).

Regarding claim 32, Utz discloses wherein the interface controller comprises a

15   network interface controller (col.7 lines 41-45; col.10 lines 48-53).

Claim Rejections - 35 USC § 103

20   **Claims 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over**

Schneier as applied to claims 1-6 above, and further in view of Alfred J. Menezes,

Paul C. van Oorschot, and Scott A. Vanstone's "Handbook of Applied

Cryptography", hereinafter referred to as *Menezes*.

Claim 8 refers to the method of claim 7, wherein act (e) comprises masking the

5   one or more bits of data into the seed pool upon termination of the second type of

triggering event.

Schneier refers only to the method of claim 7 and fails to specifically mention

masking the bits into the seed pool.

Menezes describes sampling a number of distinct sources and combining those

10   sources using a complex mixing function such as a cryptographic hashing function

(page 172 lines 34-37).

It would have been obvious to a person of average skill in the area at the time of

the invention to include within Schneier the complex mixing function as described in

Menezes to distill the true random bits from the samples sequences and guard against

15   the possibility of a few of the sources failing, or being observed or manipulated by an

adversary.

Regarding claim 9, the combined system of Schneier and Menezes further

discloses that act (e) comprises capturing the one or more bits of data from a free-

20   running timer upon termination of the second type of triggering event (Schneier page

426 lines 37-34).

Regarding claim 10, the combined system of Schneier and Menezes further

discloses that the second type of triggering event is different than the first type of

triggering event (as many good sources of randomness as are available) (Menezes

page 172 lines 32-34, 37-38).

5

Regarding claim 11, the combined system of Schneier and Menezes further

discloses that the second type of triggering event is a cycle of power applied to the

processor-based device (Schneier page 426 lines 12-13).

10   *Conclusion*

The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tamara Teslovich whose telephone number is (571)

15   272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone

number for the organization where this application or proceeding is assigned is 703-

872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

5   For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

10

T. Teslovich
June 14, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

15